UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/463,907	02/02/2000	SHIHO MORIAI	0162/00547	6943

7590 01/30/2004

POLLOCK VANDE SANDE & AMERNICK
PO BOX 19088
WASHINGTON, DC 20036-3425

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	4

DATE MAILED: 01/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/463,907	MORIAI ET AL.
	Examiner	Art Unit
	Christian La Forgia	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 02 February 2000.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-32 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-32 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 17 March 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other:

DETAILED ACTION

1. The preliminary amendment filed on 02 February 2000 is noted and made of record.

2. Claims 1 through 32 are presented for examination.

Specification

3. A substitute specification in proper idiomatic English and in compliance with 37 CFR 1.52(a) and (b) is required. The substitute specification filed must be accompanied by a statement that it contains no new matter.

4. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

5. The following title is suggested: Method and Apparatus for Evaluating the Strength of an Encryption.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1 through 12 are rejected under 35 U.S.C. 101 because they do not fall in the technological arts. Claims 1 through 12 fail to define a specific machine to produce a useful, concrete, and tangible result, and therefore are drawn to the manipulation of abstract mathematical formulas. A process that consists solely of the manipulation of an abstract idea is not concrete or tangible. See *In re Alappat*, 33 F.3d 1526, 1544, 31 USPQ2d 1545, 1557 (Fed. Cir. 1994). See *In re Warmerdam*, 33 F.3d 1354, 1360, 31 USPQ2d 1754, 1759 (Fed. Cir. 1994). See also *Schrader*, 22 F.3d at 295, 30 USPQ2d at 1459. See MPEP § 2106.

8. As per claims 1 through 12, are merely claimed as a computer program representing a computer listing *per se*, that is, descriptions or expressions of such a program and that is, descriptive material *per se*, non-functional descriptive material, and is not statutory because it is not a physical "thing" nor a statutory process, as there are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed aspects of the invention which permit the computer program's functionality to be realized. Since a computer program is merely a set of instructions capable of being executed by a computer, the program itself is not a process, without the computer-readable medium needed to realize the computer program's functionality. In contrast, a claimed computer-readable medium encoded with a computer program defines structural and functional interrelationships between the computer program and the medium which permit the computer program's functionality to be realized, and is thus statutory. *In re Warmerdam*, 33 F.3d at 1361, 31 USPQ2d at 1760. *In re Sarkar*, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106(IV)(B)(1)(a).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1 through 5, 8 through 20, and 22 through 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,825,886 to Adams et al., hereinafter Adams, in

view of **Block Ciphers – Analysis, Design and Application**, hereinafter ADA, and further in view of **Block Ciphers – A Survey**, hereinafter Survey.

11. As per claims 1 and 8, Adams teaches a function randomness evaluating apparatus comprising at least one of:

higher-order-differential cryptanalysis resistance evaluating means for calculating the minimum value of the degree of a Boolean polynomial for input bits by which output bits of a function to be evaluated are expressed, and evaluating that the larger said minimum value, the higher the resistance of said function to higher order differential cryptanalysis is (Abstract; column 3, lines 25-44; column 5, lines 3-14);

differential-linear-cryptanalysis resistance evaluating means for:

calculating, for all sets of input difference Δ x and output mask value Γ y of a function S(x) to be evaluated, the number of inputs x for which the inner product of (S(x)+S(x Δ x)) and said output mask value Γ y is 1 (Abstract; column 3, lines 25-44; column 5, lines 3-14); and

evaluating the resistance of said function to differential-linear cryptanalysis based on the result of calculation (Abstract; column 3, lines 25-44; column 5, lines 3-14). Adams, ADA, and Survey do not disclose interpolation cryptanalysis and partitioning cryptanalysis. Knudsen discusses several cryptanalysis techniques in Chapter 5 of his thesis statement, **Block Ciphers – Analysis, Design and Applications**. In particular, pages 69 through 75 discuss high-order differential cryptanalysis, pages 76 through 78 disclose partitioning cryptanalysis, and pages 80 through 88 teach differential-linear cryptanalysis. Knudsen discloses interpolation cryptanalysis on pages 35 and 36 of **Block Ciphers – A Survey**. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include interpolation and

partitioning cryptanalysis, since it has been held that forming in one piece an article which has formerly been formed in separate pieces involves only routine skill in the art. See MPEP § 2144.04; see also *Howard v. Detroit Stove Works,* 150 U.S. 164 (1994).

12. Regarding claims 2, 10, 14, 21, and 28, ADA teaches partitioning-cryptanalysis resistance evaluating means on pages 77 and 78. ADA discusses comparing the input bits to the output bits and calculating the maximum probability of matching the output bit to its respective input bit. ADA discloses differential-linear cryptanalysis resistance evaluating means on pages 82 through 85.

13. Regarding claims 3, 11, and 29, ADA teaches a similar technique for evaluating differential-cryptanalysis resistance on pages 55 through 58. ADA also discloses a technique for evaluating linear-cryptanalysis resistance on pages 84 and 85.

14. With regards to claims 4, 5, 12, 17, 24, and 30 ADA teaches similar formulas for evaluating differential-cryptanalysis resistance on pages 55 through 58. ADA also discloses similar calculations for evaluating linear-cryptanalysis resistance on pages 84 and 85.

15. As per claims 9 and 27, Adams teaches a method for evaluating the randomness of the input/output relationship of a function, said method comprising at least one of:

(a) a higher-order-differential cryptanalysis resistance evaluating step of:

letting said function be represented by S(x), calculating the minimum value of the degree of a Boolean polynomial for input bits of said function S(x) by which its output bits are expressed (column 3, lines 25-44; column 5, lines 3-14; column 10, lines 31-43); and

evaluating the resistance of said function to higher order cryptanalysis based on the result of said calculation (column 10, lines 31-43);

(b) a differential-linear cryptanalysis resistance evaluating step of:

calculating, for every set of input difference Δ x and output mask value Γ y of a function S(x) to be evaluated, the number of inputs x for which the inner product of (S(x)+S(x Δ x)) and said output mask value Γ y is 1 (column 3, lines 25-44; column 5, lines 3-14); and

evaluating the resistance of said function to differential-linear cryptanalysis based on the result of said calculation (column 10, lines 31-43). Adams, ADA, and Survey do not disclose interpolation cryptanalysis and partitioning cryptanalysis. Knudsen discusses several cryptanalysis techniques in Chapter 5 of his thesis statement, **Block Ciphers – Analysis, Design and Applications**. In particular, pages 69 through 75 discuss high-order differential cryptanalysis, pages 76 through 78 disclose partitioning cryptanalysis, and pages 80 through 88 teach differential-linear cryptanalysis. Knudsen discloses interpolation cryptanalysis on pages 35 and 36 of **Block Ciphers – A Survey**. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include interpolation and partitioning cryptanalysis, since it has been held that forming in one piece an article which has formerly been formed in separate pieces involves only routine skill in the art. See MPEP § 2144.04; see also *Howard v. Detroit Stove Works,* 150 U.S. 164 (1994).

16. As per claims 13 and 20, Adams teaches a random function generating method comprising the steps of:

(a) setting various values as each parameter for candidate functions and calculating output values corresponding to various input values (column 5, line 40 to column 6, line 9);

(b) storing the results of said calculation in storage means (column 9, lines25-36; column 10, liens 31-43); and

(c) evaluating the resistance of each of said candidate functions to a cryptanalysis based on values stored in said storage means, and selectively outputting candidate function highly resistant to said cryptanalysis (column 10, lines 31-43); and

wherein said step (c) comprising at lease one of:

(c-1) a higher-order cryptanalysis resistance evaluating step of:

calculating the minimum value of the degree of a Boolean polynomial for input bits of each of said candidate functions by which its output bits are expressed (column 3, lines 25-44; column 5, lines 3-14; column 10, lines 31-43);

evaluating the resistance of said each candidate function to higher order cryptanalysis based on the result of said calculation (column 10, lines 31-43); and

(c-2) a differential-linear cryptanalysis resistance evaluating step of:

calculating for every set of input difference Δ x and output mask value Γ y of each candidate function S(x), the number of inputs x for which the inner product of (S(x)+S(x Δ x)) and said output mask value Γ y is 1 (column 3, lines 25-44; column 5, lines 3-14; column 10, lines 31-43);

evaluating the resistance of said function to differential-linear cryptanalysis based on the result of said calculation (column 10, lines 31-43). Adams, ADA, and Survey do not disclose leaving those of said candidate functions whose resistance is higher than a predetermined second reference and discarding the others. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the selecting means, since it has been held that there is a preference for using the strongest encryption possible to avoid an unauthorized user from accessing the encrypted data. Adams, ADA, and Survey do not disclose interpolation cryptanalysis and partitioning cryptanalysis. Knudsen discusses several cryptanalysis techniques in Chapter 5 of his thesis statement, **Block Ciphers – Analysis, Design and Applications**. In particular, pages 69 through 75 discuss high-order differential cryptanalysis, pages 76 through 78 disclose partitioning cryptanalysis, and pages 80 through 88 teach differential-linear cryptanalysis. Knudsen discloses interpolation cryptanalysis on pages 35 and 36 of **Block Ciphers – A Survey**. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include interpolation and partitioning cryptanalysis, since it has been held that forming in one piece an article which has formerly been formed in separate pieces involves only routine skill in the art. See MPEP § 2144.04; see also *Howard v. Detroit Stove Works,* 150 U.S. 164 (1994).

17. Regarding claims 15, 18, 22, and 25, Adams, ADA, and Survey do not teach when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said reference by a predetermined width, and executing again the evaluation and selecting process. Adams discloses proving the resistance of a generated function using

differential and linear cryptanalysis, see column 10, lines 31-43. Adams, ADA, and Survey do not disclose easing the candidate function selecting condition by changing said reference by a predetermined width, and executing again the evaluation and selecting process when all the candidate functions have been discarded. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a selection process, since it has been held that there is a preference for using the strongest encryption possible to avoid an unauthorized user from accessing the encrypted data.

18. Regarding claims 16 and 23, ADA teaches a similar technique for evaluating differential-cryptanalysis resistance on pages 55 through 58. ADA also discloses a technique for evaluating linear-cryptanalysis resistance on pages 84 and 85. Adams, ADA, and Survey do not disclose leaving those of said candidate functions whose resistance is higher than a predetermined second reference and discarding the others. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the selecting means, since it has been held that there is a preference for using the strongest encryption possible to avoid an unauthorized user from accessing the encrypted data.

19. Regarding claims 19, 26, 31, and 32, Adams teaches wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function (column 6, line 63 to column 7, line 30).

20. Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adams.

21. As per claim 6, Adams teaches a random function generating apparatus comprising:

candidate function generating means for generating candidate functions each formed by a combination of a plurality of functions of different algebraic structures and having a plurality of parameters (Figure 2; column 5, lines 40-66; column 6, line 63 to column 7, line 31);

resistance evaluating means for evaluating the resistance of each of said candidate functions to a cryptanalysis (column 5, lines 3-23; column 10, lines 31-43); and

selecting means for selecting those of said resistance-evaluated candidate functions which have highly resistant to said cryptanalysis (column 10, lines 31-43). Adams discloses proving the resistance of a generated function using differential and linear cryptanalysis, see column 10, lines 31-43. Adams, ADA, and Survey do not disclose selecting those of said resistance-evaluated candidate functions which have highly resistant to said cryptanalysis. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the selecting means, since it has been held that there is a preference for using the strongest encryption possible to avoid an unauthorized user from accessing the encrypted data.

22. Regarding claim 7, Adams teaches wherein one of said plurality of functions of different algebraic structures is resistant to each of differential cryptanalysis and linear cryptanalysis (column 5, lines 3-23).

Conclusion

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

24. The following patents are cited to further show the state of the art with respect to cryptanalysis, such as:

United States Patent No. 6,504,929 to Tsunoo, which is cited to show an encryption strength evaluation method that teaches away from the instant application by stating that the invention cannot evaluate using a method that depends upon linear decoding.

United States Patent No. 6,314,186 to Lee et al., which is cited to show robust security against differential, linear, and high-order differential cryptanalysis.

United States Patent No. 6,031,911 to Adams et al., which is cited to show a practical s-box design.

United States Patent No. 5,745,577 to Leech, which is cited to show a symmetric cryptographic system.

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

26. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 746-7240.

27. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Christian LaForgia
Patent Examiner
Art Unit 2131

Clf 1

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100